«Утверждаю»
Директор ТОО «МФО Взаймы»
_____ Гребенников П.А.
Приказ №___ от «___» марта 2020г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ И ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОННИРОВАННОГО ДОСТУПА ПРИ ПРЕДОСТАВЛЕНИИ УСЛУГ ПОСРЕДСТВОМ ИНТЕРНЕТ-РЕСУРСА, МОБИЛЬНОГО ПРИЛОЖЕНИЯ И (ИЛИ) ТЕРМИНАЛА В ТОО «МФО «ВЗАЙМЫ»

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Политика безопасности и защиты информации от несанкционированного доступа при предоставлении услуг посредством интернет-ресурса, мобильного приложения и (или) терминала в ТОО «МФО «Взаймы» (далее - Политика) разработана в соответствии с нормами действующего законодательства Республики Казахстан в сфере информационной безопасности, Актами уполномоченного органа и внутренними документами ТОО «МФО «Взаймы» (далее - МФО).

2. Основной целью Политики, является минимизация ущерба от событий, таящих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму. Информационная безопасность не является самоцелью, ее обеспечение необходимо для снижения рисков и экономических потерь, связанных со всевозможными угрозами имеющимся информационным ресурсам МФО. С этой целью необходимо поддерживать главные свойства информации, а именно:

- доступность – свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия;
- конфиденциальность – свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;
- целостность – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

3. Основными принципами Политики являются:

- законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации МФО;
- ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки основной деятельности. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий деятельности МФО;
- непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты МФО должны осуществляться без прерывания или остановки текущих бизнес-процессов МФО;
- комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;
- обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем информационной безопасности должна быть меньше размера возможного ущерба от любых видов риска;

- приоритетность – категорирование (ранжирование) всех информационных ресурсов МФО по степени важности при оценке реальных, а также потенциальных угроз информационной безопасности.

4. Настоящая Политика определяет:
   - Основные меры по обеспечению информационной безопасности МФО
   - способы многофакторной аутентификации и верификации потенциальных заемщиков посредством интернет-ресурса, мобильного приложения и (или) терминала;
   - обеспечение безопасного хранения электронных сообщений и иных документов, предоставленных заемщику и полученных от него, с соблюдением их целостности и конфиденциальности в течение не менее 5 (пяти) лет после прекращения обязательств сторон по договору о предоставлении микрокредита;
   - меры для профилактики замышляемых правонарушений со стороны третьих лиц.

5. Настоящая Политика обязательна для исполнения всеми работниками МФО, стажерами, практикантами, а также должна доводиться до сведения заемщиков и иных третьих лиц, имеющих доступ к информационным системам и документам МФО, в той их части, которая непосредственно взаимосвязана с МФО и их деятельностью.

6. Процесс создания надежной информационной защиты никогда не бывает законченным. В целях обеспечения достаточно надежной системы информационной безопасности, необходима постоянная регулировка ее параметров, адаптация для отражения новых опасностей, исходящих из внешней и внутренней среды.

ГЛАВА 2. МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7. Основными мерами по обеспечению информационной безопасности МФО являются:
   - административно-правовые и организационные меры;
   - меры физической безопасности;
   - программно-технические меры.

7.1. Административно-правовые и организационные меры включают (но не ограничены ими):
   - контроль исполнения требований законодательства РК и внутренних документов;
   - разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;
   - контроль соответствия бизнес-процессов требованиям Политики;
   - информирование и обучение работников МФО работе с информационными системами и требованиям информационной безопасности;
   - реагирование на инциденты, локализацию и минимизацию последствий;
   - анализ новых рисков информационной безопасности;
   - отслеживание и улучшение морально-делового климата в коллективе;
   - определение действий при возникновении чрезвычайных ситуаций;
   - проведение профилактических мер при приеме на работу и увольнении работников МФО.

7.2. Меры физической безопасности включают (но не ограничены ими):
   - организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;
   - организацию противопожарной безопасности охраняемых объектов;
   - контроль доступа работников МФО в помещения ограниченного доступа (сервер).

7.3.Программно-технические меры включают (но не ограничены ими):

- использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
- использование средств защиты периметра (firewall, IPS и т.п.);
- применение комплексной антивирусной защиты;
- использование средств информационной безопасности, встроенных в информационные системы;
- обеспечение регулярного резервного копирования информации;
- контроль за правами и действиями пользователей, в первую очередь, привилегированных;
- применение систем криптографической защиты информации;
- обеспечение безотказной работы аппаратных средств.

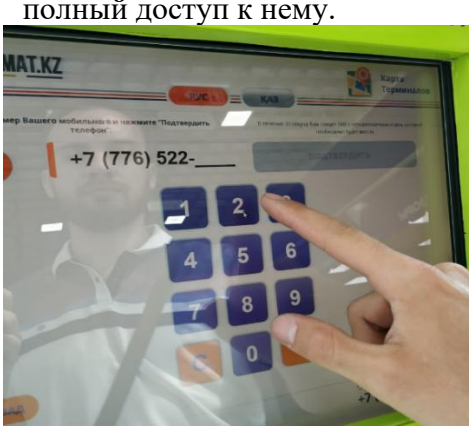
ГЛАВА 3. БИЗНЕС ПРОЦЕСС МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ И ВЕРИФИКАЦИИ ПОСРЕДСТВОМ ТЕРМИНАЛА

8. Многофакторная аутентификации и верификации посредством терминала включает в себя:

- Смс-сообщение;
- Сканирование документа личности, в трех цветовых диапазонах;
- Биометрия лица, пальца потенциального заемщика;
- Видеосъёмка получения микрозайма.

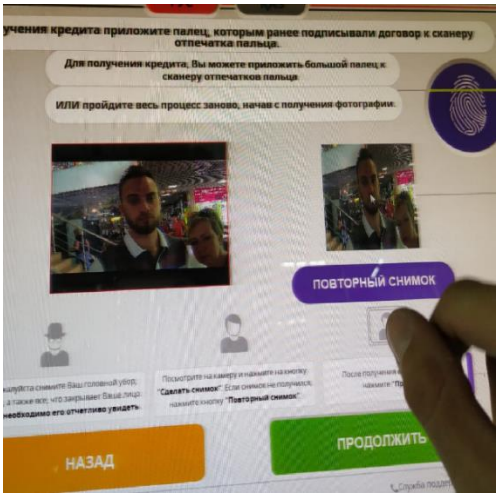
9. Бизнес процесс многофакторной аутентификации и верификации посредством терминалов осуществляется следующим образом:

9.1. Терминал запрашивает номер телефона потенциального заемщика, для отправки смс-сообщения с уникальным кодом, который действует в течение 1-ой минуты. Код в свою очередь вводится в терминал, тем самым активирует терминал к дальнейшей работе. Данное действие подтверждает, что заемщик имеет при себе данный номер и имеет полный доступ к нему.

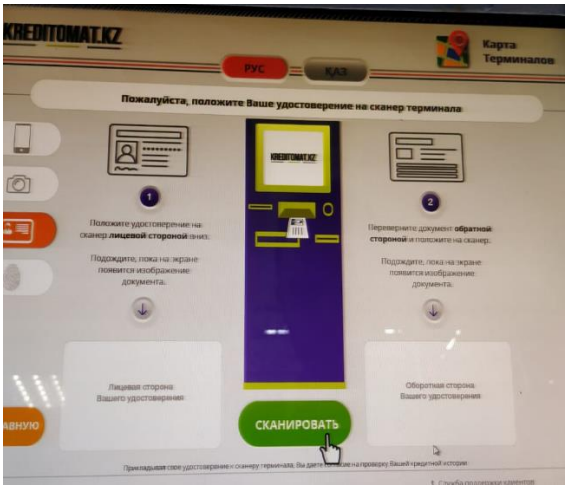


9.2. После активации терминала, потенциальному заемщику необходимо сфотографироваться, обязательно направив взгляд на камеру. При этом, необходимо снять очки и головной убор.

В момент получения фотографии производится видеосъемка лица потенциального заемщика и идет поиск изменении показателей мимики в биометрии лица перед терминалом и сравниваются общие биометрические особенности лица в видео с фотографией. Это служит доказательством того что полученная фотография клиента сделана в терминале с образа живого, двигающегося человека.



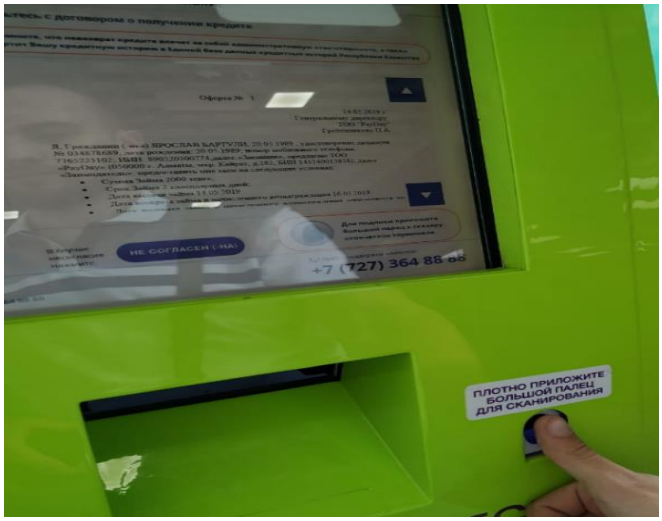
9.3. Следующим действием осуществляется сканирование удостоверения личности. Документ (удостоверение личности) помещается на стекло сканера и сканируется с двух сторон.



9.4. После получения изображения документа (удостоверения личности) клиента, терминал осуществляет проверку его подлинности на соответствие всех степеней защиты в ультрафиолетовом и инфракрасном спектре, а также водяные знаки, согласно требованиям законодательства Республики Казахстан. Распознавание ключевых данных, таких как ИИН гарантируется наличием проверочной цифры в зоне MRZ документа.

9.5. В случае наличия отклонения от запрограммированных степеней идентификации, терминал помечает данную заявку как сомнительную и направляет на дополнительную проверку к верификаторам.

9.6. При этом, одновременно осуществляется автоматическое сравнение биометрии лица и пальца потенциального заемщика.



9.7. В случае получения наличных денежных средств через Терминал, в момент выдачи Заемщикуденежных средств, ведется запись двумя камерами, установленными в отсеке выдачи купюр и в верхней части терминала. Это служит дополнительным доказательством, того что прошедший идентификацию заемщик, получил запрашиваемые средства.

9.8. После получения вышеуказанной информации, терминал сравнивает:

- биометрию лица (фото) потенциального заемщика среди биометрии (фото) лиц других клиентов;
- номера ИИН, ФИО и т.д.;

9.9. В случае нахождения идентичной биометрии, ИИН и т.д. среди клиентской базы, заявка потенциального заемщика помечается как сомнительная и передается в работу верификаторам с указанием клиента на которого похож потенциальный заемщик.

9.10. Сомнительная заявка отправляется двум специально обученным верификаторам одновременно для анализа (согласно Должностной инструкции, Регламента работы отдела верификации). Анализ согласно Регламента работы осуществляется в течение 30 секунд, с момента поступления заявки:

9.10.1. изображения документа (удостоверение личности) в ультрафиолетовом спектре, определяя имеются ли водяные знаки и почему их плохо видно (грязь, потертость на документе и т.п.);

9.10.2. биометрии лица (фото) потенциального заемщика, в случае если потенциальный заемщик сильно поправился, похудел или постарел;

9.10.3. биометрии лица (фото) потенциального заемщика среди биометрии (фото) лиц других клиентов, т.е. потенциальный заемщик до текущей заявки уже обращался в МФО для получения кредита под другим документом (удостоверением личности).

9.11. В случае если верификаторы одновременного принимают положительное решение по сомнительной заявке, потенциальному клиенту одобряется микрокредит (Схема №1).

9.12. В случае если один из верификаторов отклонил сомнительную заявку, потенциальному заемщику поступает отказ в оформлении микрокредита (Схема №2).

9.13. Сомнительные заявки не прошедшие ручную верификацию вносится автоматически в черный список, и в последующем при повторном обращении данного лица в МФО, система сразу же отображает на дисплее терминала отказ в оформлении микрокредита.

9.14. Кроме того, руководитель отдела верификации на еженедельной основе производит мониторинг отклоненных заявок, в части соблюдения должностной инструкции верификаторами и выявления мошеннических действии со стороны потенциальных заемщиков, с целью модернизации (улучшения) технологических процессов МФО.

Схема №1

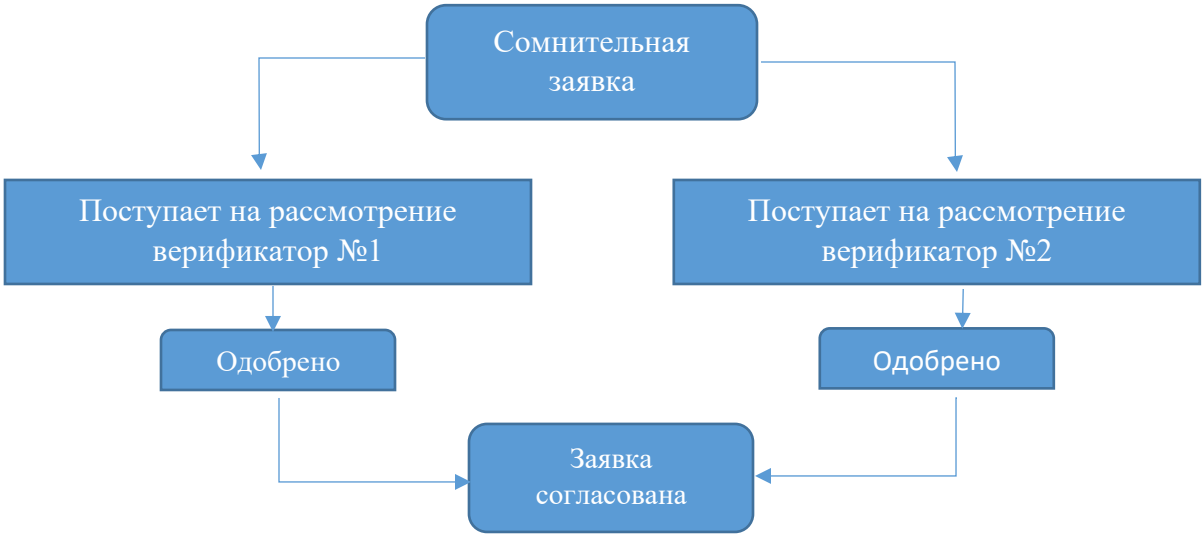
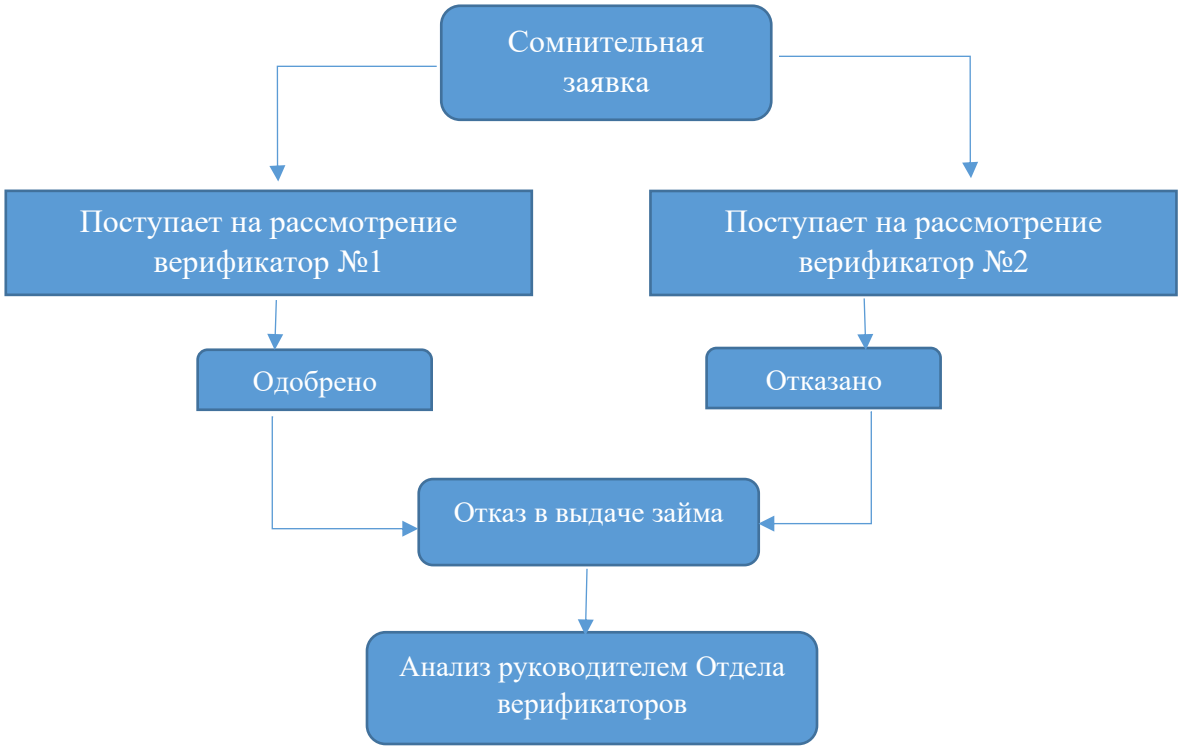


Схема №2



ГЛАВА 4. БЕЗОПАСНОЕ ХРАНЕНИЕ ЭЛЕКТРОННЫХ СООБЩЕНИЙ И ИНЫХ ДОКУМЕНТОВ

10. В целях обеспечения информационной безопасности МФО выполняются следующие условия:

- по организации системы управления информационной безопасностью;
- по организации доступа к информационным активам;
- по обеспечению безопасности информационной инфраструктуры;
- по осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;
- по проведению анализа информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах;
- по средствам криптографической защиты информации;
- по обеспечению информационной безопасности при доступе третьих лиц к информационным активам;
- по проведению внутренних проверок состояния информационной безопасности;
- по процессам системы управления информационной безопасностью.

11. Подлежащая защите информация может:

- размещаться на бумажных носителях;
- существовать в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники, записываться и воспроизводиться с помощью технических средств);
- передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;
- присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров.

12. Требования к обеспечению информационной безопасности при организации деятельности МФО в части договоров на предоставление сведений о потенциальных заемщиках (данные об официальных доходах, перечислениях из ГФСС, о количестве и средней сумме пенсионных выплат из республиканского бюджета, данных кредитного отчета и другие отчеты) от ТОО «Первое кредитное бюро» (далее – ПКБ) в рамках заключенных договоров**:**

12.1. МФО обеспечивает конфиденциальность и целостность информации, получаемой из информационной системы ПКБ.

12.2. МФО обеспечивает надлежащий уровень информационной безопасности в соответствии с условиями Договоров, заключенных с ПКБ.

12.3. МФО обеспечивает исполнение организационно-технических, технологических требований и мер, необходимых для функционирования и защиты системного и прикладного программного обеспечения, используемого для взаимодействия с информационной системой ПКБ и обработки получаемой из нее информации.

12.4. При использовании оборудования для работы с информационной системой ПКБ учитывается необходимость его защиты от несанкционированного доступа, а также защиты носителей информации и сетевых ресурсов, используемых для работы с информационной системой ПКБ.

12.5. МФО определяет и утверждает перечень ответственных лиц.

12.6. МФО обеспечивает наличие подписанных ответственными (ответственным) лицами (лицом) организации обязательств о неразглашении и нераспространении информации, ставшей им известной в процессе исполнения ими функциональных обязанностей.

12.7. МФО обеспечивает наличие внутренних документов, определяющих порядок определения и утверждения перечня ответственных лиц, их права и ответственность (включая должностные инструкции).

12.8. Доступ к информации предоставляется работникам МФО в объеме, необходимом для исполнения их функциональных обязанностей.

12.9. Учетная запись ответственного лица, по которой он идентифицируется в информационной системе ПКБ, соответствует конкретному физическому лицу.

12.10. МФО проводит плановые и внеплановые проверки соответствия рабочих станций (терминалов, мобильных приложений, сайта) Политике информационной безопасности.

12.11. МФО по запросу уполномоченного органа представляет сведения, подтверждающие его соответствие требованиям, предусмотренным в договорах с ПКБ.

12.12. Операционная система рабочей станции обеспечивает функции идентификации и аутентификации пользователя, а также разграничения прав доступа пользователей и авторизации в соответствии с назначенными правами.

12.13. МФО использует собственную рабочую станцию.

12.14. При использовании рабочей станции для подключения к информационной системе Кредитного бюро одновременное подключение к другим ресурсам сети интернет не производится.

12.15. Работники МФО обеспечивают конфиденциальность персональных идентификационных и аутентификационных данных, используемых для доступа к информационным системам.

12.16. Работники МФО обеспечивают конфиденциальность информации, ставшей им известной в процессе использования информационной системы Кредитного бюро.

13. Ответственность за обеспечение информационной безопасности МФО возлагается на все структурные подразделения МФО в рамках их полномочий и в соответствии с положениями, установленными настоящей Политикой и разработанными на ее основе документами.

14. За нарушение требований настоящей Политики и документов, разработанных на ее основе, предусмотрена ответственность в соответствии с внутренними нормативными документами МФО и законодательством РК.

ГЛАВА 5. МЕРЫ ПРОФИЛАКТИКИ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ

15. В профилактике инцидентов кибербезопасности важную роль играет соблюдение соответствующих национальных и международных требований при разработке программного обеспечения, проектировании компонентов информационных систем и инфраструктуры финансового сектора. МФО выполняет регулярную оценку рисков кибербезопасности, которая служит основой для выработки и применения мер по минимизации данных рисков, а также оценки эффективности реализованных мер.

16. Учитываются результаты, полученные на этапе профилактики (предотвращения), а также опыт уже обработанных инцидентов. Своевременно оценивается характер, масштабы и последствия инцидентов кибербезопасности, в целях снижения результатов их воздействия,

своевременно уведомляются внутренние и внешние заинтересованные стороны и координируются совместные действия по реагированию. К заинтересованным сторонам относятся:

- Национальный Банк Республики Казахстан;
- иные уполномоченные государственные и законодательные органы, осуществляющие регулирование деятельности МФО;
- заемщики;
- кредиторы и инвесторы;
- работники структурных подразделений, осуществляющие взаимодействие в процессе осуществления деятельности МФО;
- поставщики услуг.

17. Обеспечивается продолжение операционной деятельности после инцидента при одновременном выполнении процедур восстановления, в том числе:

- устранения последствий инцидента;
- восстановления нормального состояния информационных систем и данных с подтверждением их нормального состояния;
- выявления и устранения уязвимостей, которые были использованы в рамках инцидента, в целях недопущения подобных инцидентов в будущем;
- обеспечения надлежащего информационного обмена внутри страны и за ее пределами.

18. Повышение информированности и компетенции, как пользователей, так и работников (повышение квалификации, обучение) помогут устранить риски и создать культуру безопасного создания и использования информации в МФО. На этапе повышения осведомленности следует использовать опыт, полученный в ходе профилактики и реагирования, чтобы пользователи были ознакомлены с реальными рисками и эффективными методами их минимизации.

19. В случае обнаружения несанкционированного доступа к информации, составляющей тайну предоставления микрокредита, ее несанкционированного изменения, осуществления несанкционированных действий со стороны третьих лиц, МФО незамедлительно принимает меры для устранения причин и последствий таких действий, а также в течение одного рабочего дня информирует об этом уполномоченный орган.

20. МФО принимает меры по предотвращению использования действующих или внедряемых способов и технологий предоставления микрокредитов электронным способом в схемах легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма. При предоставлении микрокредитов и проведении кредитного скорринга потенциального заемщика МФО применяет необходимые меры, предусмотренные Законом Республики Казахстан от 28 августа 2009 года «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Закон о ПОДФТ), а также в соответствии с Постановлением Правления Национального Банка Республики Казахстан О внесении изменений и дополнений в постановление Правления Национального Банка Республики Казахстан от 25 декабря 2013 года № 292 "О введении ограничений на проведение отдельных видов банковских и других операций финансовыми организациями".

ГЛАВА 6. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В НАСТОЯЩУЮ ПОЛИТИКУ

20.1. Предложения о внесении изменений и дополнений в настоящую Политику могут быть инициированы любым сотрудником МФО посредством предоставления их в письменном виде директору МФО.

20.2. Внесение изменений и дополнений в настоящую Политику производятся в соответствии с изменениями в Законодательстве Республики Казахстан и при необходимости.